UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,150	05/14/1999	PHILIP J. MIRE	M-7219-US	2203

7590 11/12/2003

DAVID L. McCOMBS
HAYNES and BOONE, LLP
901 MAIN STREET
SUITE 3100
DALLAS,, TX 75202-3789

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/312,150	MIRE, PHILIP J.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) *2,3,6,13,14,17,24 and 25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,5,7-12,15,16,18-23 and 26-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 May 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-29 are pending in the application.

2. Claims 2, 3, 6, 13, 14, 17, 24 and 25 have been cancelled.

Response to Amendment

3. The examiner approves the new title.

4. The examiner still disapproves the drawings.

Response to Arguments

5. Applicant's arguments filed 9/4/036 have been fully considered but they are not persuasive.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

In this case, the use of public/private keys and their benefits are well known in the art. Therefore it is beneficial to make the user and master keys public/private key pairs.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 7 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 7 depends upon claim 2. Claim 2 is a cancelled claimed. A claim cannot depend upon a claim that has been cancelled. For the sake of examining, the examiner assumes that claim 7 depends upon claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 4, 5, 7, 8, 12, 15, 16, 18, 19, 23 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burke et al U.S. Patent No. 5,706,347 in view of Applied Cryptography (hereinafter Schneier).

As to claims 1, 4, 12, 15, 23, 26 and 28, Burke et al discloses generating a session key. Burke et al discloses encrypting the data utilizing the session key. Burke et al discloses

encrypting the session key utilizing a user's key. Burke et al discloses encrypting the session key utilizing a master key. Burke et al discloses generating a data packet including the encrypted data and the encrypted session keys. Burke discloses an authorized party accessing the encrypted data by utilizing the master key. Burke discloses that the authorized party decrypts the encrypted session key utilizing the master key and decrypting the encrypted data with the session key to recreate original data.

Burke et al does not teach that the user key encrypting the session is a public key. Burke et al does not teach that the master key encrypting the session is a public key. Burke et al does not teach that the authorized party accesses the encrypted data using a master public and private key. Burke et al does not teach that the session key that is decrypted with the master key is a private key.

Schneier teaches public-key management and its benefits and asymmetric encryption routines [pages 185-187].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burke et al so that the master key and the user's key were both public keys that are used to encrypt the session keys. The keys included in the data packet would have been encrypted with a user public key and a master public key. The session keys would have been encrypted using asymmetric routines.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burke et al by the teaching of Schneier because it would have been that a private key of the public-private key pair authenticates a relationship as well as an identity [page 186].

As to claims 5, 16 and 27, Burke et al discloses encrypting the data utilizing a symmetric encryption routine. The examiner asserts that since the same session key is used to encrypt and decrypt data, as taught by Burke, thus symmetric encryption is being utilized.

As to claims 7 and 18, the Burke et al teaches storing the user's private key on a storage medium coupled to the destination data processing system [element **11** of figure 1 of Lennon et al U.S. Patent No. 4,193,131 incorporated by reference to Burke et al]. The examiner asserts that since public-key encryption was being used the user's private key has to be stored at the destination processing system in order to decrypt the session key.

As to claims 8 and 19, the Burke et al teaches storing the master private key on a data storage medium coupled to the destination data processing system [element **11** of figure 1 of Lennon et al U.S. Patent No. 4,193,131 incorporated by reference to Burke et al].

8. Claims 9, 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burke et al U.S. Patent No. 5,706,347 and Schneier as applied to claims 1 and 12 above, and further in view of Dillaway et al U.S. Patent No. 5,742,756.

As to claims 9 and 20, the Burke-Schneier combination does not teach retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [column 3, lines 24-31].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the user's

private key is stored on a smart card coupled to the destination node. The private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination by the teaching of Dillaway because in using a smart Card to perform critical cryptography operations. The smart Card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart Card, and required cryptographic operations are performed on the smart Card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claims 10 and 21, the Burke-Schneier combination does not teach retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [column 3, lines 24-31].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the master private key is stored on a smart card coupled to the destination node. The master private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination by the teaching of Dillaway because in using a smart card to perform critical cryptography operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather

than providing a private key to the user's computer, the key is held within the smart card, and required cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

9. Claims 11, 22 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burke et al U.S. Patent No. 5,706,347 and Schneier as applied to claims 1, 12 and 23 above, and further in view of Kruys U.S. Patent No. 5,555,309.

As to claims 11 and 29, the Burke-Schneier combination does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination by the teaching of Kruys is that master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

As to claim 22, the Burke-Schneier combination teaches decrypting the data with the session key, as discussed above.

The Burke-Schneier combination does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

The motivation to have modified the Burke-Schneier combination by the teaching of Kruys is that master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy
November 4, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100